Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to activate at least part of its functionality;

~~requiring a user to enter into the user's computer identifying data that identifies the user;~~

requiring the user to communicate user data over a communications network to a remote service provider ~~system~~, the user data being derived, at least in part, from ~~the identifying data that identifies the user, and being derived, at least in part, from~~ the unique identification code;

~~archiving user data received from the user over the communications network in a data storage element of the remote service system, said remote service system being connected to said communications network and designated to receive said user data;~~

~~comparing~~ examining received user data ~~for each~~ to derive the unique identification code associated with the copy of the software application installed by said user ~~with previously archived user data corresponding to the same unique identification code to determine whether said user is pirating~~

counting the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code; and

selectively transmitting service data to the user's computer ~~from said remote service system~~ when said remote service provider ~~system~~ determines that ~~said service data should be transmitted~~ the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code is fewer than a predetermined threshold, said user's computer being connected to said

communications network and designated to storably receive said service data.

2. Canceled.

3. (Previously presented) The method as in Claim 1,

wherein said user data comprises the unique identification code that identifies said software application installed on a data storage element of the user's computer.

4. (Previously presented) The method as in Claim 1,

wherein said user data includes ~~said~~ identifying data that identifies the user.

5. (Previously presented) The method as in Claim 1,

wherein said user data includes product information relating to said software application installed on the data storage element of the user's computer.

6. Canceled.

7. Canceled.

8. Canceled.

9. Canceled.

10. Canceled.

11. Canceled.

12. (Currently amended) The method as in Claim 1,

wherein said service data is maintained in the data storage element of the remote service provider ~~system~~.

13. (Previously presented) The method as in Claim 12,

wherein said service data comprises at least one program code sequence that activates at least part of the functionality of said software application stored on said data storage element of the user's computer.

14. (Previously presented) The method as in Claim 12,

wherein said service data includes at least one program code sequence that results in a promotional message that may be displayed to said user on the user's computer system.

15. Canceled.

16. Canceled.

17. Canceled.

18. (Currently amended) The method as in Claim 1,

wherein said service data is derived at least in part from said user data stored on said data storage element of said remote service provider ~~system~~.

19. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is an uploading event in which said service data is automatically transferred from said remote service provider ~~system~~ and storably received by the user's computer system.

20. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is an uploading event in which said service data is manually transferred from said remote service provider ~~system~~ and storably received by the user's computer system.

21. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is a downloading event in which said service data is made available to said user from said remote service provider ~~system~~, and wherein said user downloads said service data into the user's computer system.

22. (Previously presented) The method as in Claim 1,

wherein said software application includes a program code sequence that identifies said software application stored on said data storage element of the user's computer system, said software application additionally being responsive to a second program code sequence that activates at least part of the functionality of said software application, and which is transmitted to the user's computer system via said communications network.

23. (Currently Amended) A system for preventing piracy of a given software application, said software application having a unique identification code associated therewith, and said software application requiring service data to activate at least part of the functionality of said software application, said system comprising:

a user computer system on which a user desires to operate the software application, said user system being connected to a communications network to transmit user data and to ~~storably~~ receive said service data, said user data being derived at least in part from ~~identifying data entered by the user on the user computer system which identifies the user, and being derived at least in part from~~ said unique identification code;

a remote service computer system connected to said communications network to ~~storably~~ receive user data transmitted over the communications network from the user computer system said remote service computer system transmitting said service data to said user computer system ~~over~~

~~said communications network~~ when ~~it is determined that said user is not pirating~~ the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code is fewer than a predetermined threshold.

24. (Previously presented) The system as in Claim 23

wherein said remote service computer system includes a data storage element for archiving user data for each unique identification code, wherein said remote service computer system compares user data received from the user computer system to user data previously archived by said remote service computer system relative to the same unique identification code, and wherein said remote service computer system transmits said service data to said user computer system when said user data received by said remote service computer system is consistent with user data previously archived by said remote service computer system relative to the same unique identification code.

25. (Previously presented) The system as in Claim 23

wherein said service data is maintained by said remote service computer system in the data storage element used to archive said service data.

26. (Previously presented) The system as in Claim 23

wherein said service data consists, at least in part, of an activation code sequence to activate at least part of the functionality of the software application.

27. (Currently amended) The system as in Claim 23

wherein said service data is ~~automatically~~ transferred by said remote service computer system without human intervention and ~~storably~~ received by said user computer system.

28. (Previously presented) The system as in Claim 23

wherein said remote service computer system manually transfers said service data from said remote service computer system to said user system.

29. (Previously presented) The system as in Claim 23

wherein said remote service computer system makes said service data available to said user from said remote service system, said user being able to download said service data into said user computer system.

30. (Previously presented) The system as in Claim 23,

wherein said software application includes a program code sequence that identifies said software application stored on said data storage element of said user system, said software application additionally being responsive to a second program code sequence that activates at least part of the functionality of said software application, and which is transmitted to said user system via a communications network.

31. (Currently amended) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to activate at least part of its functionality ;

~~requiring a user to enter into the user's computer identifying data that identifies the user;~~

requiring the user to communicate user data over a communications network to a remote service provider ~~system~~, the user data being derived, at least in part, from ~~the identifying data that identifies the user, and being derived, at least in part, from~~ the unique identification code;

examining received user data ~~received by the remote service system from the user's computer~~ to ~~determine whether the user is pirating~~ derive the unique identification code associated with said ~~the~~ software application;

determining the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code;

selectively transmitting service data to the user's computer ~~from said remote service system~~ when ~~said remote service system determines that the user is not pirating the software application~~ the number of times an attempt has been made to obtain said service data is fewer than a predetermined threshold; and

~~storably~~ receiving the transmitted service data within ~~the data storage element of~~ the user's computer, wherein said service data is used to activate at least part of the functionality of the software application.

32. (Previously presented) The method recited by Claim 31 further including the step of archiving user data received from users over the communications network in a data storage element of the remote service system.

33. (Previously presented) The method recited by Claim 32,

wherein received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

34. (Previously presented) The system as recited in Claim 26,

wherein said service data includes at least one program code sequence that results in a promotional message that may be displayed to said user on said user computer system.

35. (Currently amended) A method of preventing piracy of a given software application comprising the steps of:

a. assigning a unique identification code to each authentic copy of such software application;

b. installing the software application in a data storage element on a user's computer;

c. configuring the software application to require service data ~~to activate~~ , said service data being a necessary component to enable at least part of ~~its~~ the software's functionality;

d. requiring the user to communicate user data to a remote service provided ~~system~~, the user data being derived, at least in part, from ~~identifying data that identifies the user, and being derived, at least in part, from~~ the unique identification code;

e. examining received user data ~~received by the remote service system~~ to ~~determine whether the user is pirating~~ derive the unique identification code associated with said ~~the~~ software application;

f. determining the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code;

g. selectively transmitting service data to the user's computer ~~from said remote service system~~ when ~~said remote service system determines that the user is not pirating~~ the number of times an attempt has been made to obtain said service data in order to activate the software application assigned to such unique identification code is fewer than a predetermined threshold; and

~~g.~~ h. ~~storably~~ receiving the transmitted service data within ~~the data storage element of~~ the user's computer, wherein said service data is used to activate at least part of the functionality of the software.

36. (Previously presented) The method recited by Claim 35 further including the step of archiving user data received from users.

37. (Previously presented) The method recited by Claim 36,

wherein received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

38. (Currently amended) A method of preventing piracy of a given software application

comprising the steps of:

a. assigning a unique identification code to each authentic copy of such software application;

b. installing the software application in a data storage element on a user's computer;

c. configuring the software application to require service data, said service data being a necessary component to enable at least part of the software's functionality;

d. requiring the user to communicate user data to a ~~remote~~ service provider ~~system~~, the user data being derived, at least in part, from ~~identifying data that identifies the user, and being derived, at least in part, from~~ the unique identification code;

e. examining received user data ~~received by the remote service system~~ to ~~determine whether the user is pirating~~ derive the unique identification code associated with said ~~the~~ software application;

f. ascertaining the number of times an attempt has been made to obtain said service data in order to activate at least part of the functionality of said software application assigned to such unique identification code ~~selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that the user is not pirating the software application~~; and

g. determining whether the number of times an attempt has been made to obtain said service data is fewer than a predetermined threshold ~~storably receiving the transmitted service data within the data storage element of the user's computer to activate at least part of the software's functionality~~ .

39. (Previously presented) The method recited by Claim 38 further including the step of archiving user data received from users.

40. (Previously presented) The method recited by Claim 39,

wherein received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

41. (New) The method recited by Claim 31 wherein said received service data is stored within the data storage element of the user's computer.

42. (New) The method recited by Claim 35, wherein said received service data is stored within the data storage element of the user's computer.

43. (New) The method recited by Claim 38 further including the step of communicating service data to the user to activate at least part of the said software's functionality.

44. (New) The method recited by Claim 43, wherein said communicated service data is stored within the data storage element of the user's computer.

45. (New) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to activate at least part of its functionality;

requiring the user to communicate user data to a remote service provider, the user data being derived, at least in part, from the identifying data that identifies the user, and being derived, at least in part, from the unique identification code;

archiving identifying data received from a user for each unique identification code if no such identifying data has previously been archived for such unique identification code;

comparing received identifying data associated with a unique identification code with previously archived identifying data corresponding to the same unique identification code if such identifying data has previously been archived;

selectively transmitting service data to the user's computer when no such identifying data has previously been archived for such unique identification code;

selectively transmitting service data to the user's computer when the received identifying

data is consistent with previously archived data for the same unique identification code; and

receiving the transmitted service data within the data storage element of the user's computer to activate at least part of the functionality of the software application.

46. (New) The method recited by claim 45 wherein said step of selectively transmitting service data to the user's computer when the received identifying data is consistent with previously archived data for the same unique identification code includes the steps of:

a. determining the number of times that said service data has been requested; and

b. refusing transmission of said service data when the number of times that said service data has been requested exceeds a predetermined threshold.

47. (New) The method recited by claim 45 including the steps of:

a. determining the number of times that received identifying data is not consistent with previously archived data for the same unique identification code; and

b. refusing transmission of said service data when the number of times that received identifying data is not consistent with previously archived data for the same unique identification code exceeds a predetermined threshold.

48. (New) The method recited by Claim 45 further including the step of archiving identifying data received from a user for each unique identification code subsequent to an initial archiving of identifying data pertaining to the same unique identification code.

49. (New) The method recited by Claim 45 wherein said received service data is stored within the data storage element of the user's computer.

50. (New) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to activate at least part of its functionality;

requiring the user to communicate user data to a service provider, the user data being derived, at least in part, from the identifying data that identifies the user, and being derived, at least in part, from the unique identification code;

archiving identifying data received from a user for each unique identification code if no such identifying data has previously been archived for such unique identification code;

comparing received identifying data associated with a unique identification code with previously archived identifying data corresponding to the same unique identification code if such identifying data has previously been archived;

determining if identifying data has previously been archived for such unique identification code, and if so, whether such previously archived data is consistent with newly-received identifying data for the same unique identification code.

51. (New) The method recited by Claim 50 further including the step of communicating service data to the user to activate at least part of the said software's functionality.

52. (New) The method recited by Claim 51, wherein said communicated service data is stored within the data storage element of the user's computer.

53. (New) The method recited by claim 50 wherein said step of communicating service data to the user further includes the steps of:

a. determining the number of times that said service data has been requested; and

b. refusing transmission of said service data when the number of times that said service data has been requested exceeds a predetermined threshold.

54. (New) The method recited by Claim 50 further including the step of archiving identifying data received from a user for each unique identification code subsequent to an initial archiving of

identifying data pertaining to the same unique identification code.

55. (New) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to activate at least part of its functionality;

requiring the user to communicate user data to a service provider, the user data being derived, at least in part, from the identifying data that identifies the user, and being derived, at least in part, from the unique identification code;

comparing received identifying data associated with a unique identification code with previously archived identifying data corresponding to the same unique identification code if such identifying data has previously been archived;

selectively communicating service data to the user when the received identifying data is consistent with previously archived data for the same unique identification code; and

receiving the communicated service data wherein said service data is used to activate at least part of the functionality of the software.

56. (New) The method recited by claim 55 wherein said step of selectively communicating service data to the user when the received identifying data is consistent with previously archived data for the same unique identification code includes the steps of:

a. determining the number of times that said service data has been requested; and

b. refusing communication of said service data when the number of times that said service data has been requested exceeds a predetermined threshold.

57. (New) The method recited by claim 55 including the steps of:

a. determining the number of times that received identifying data is not consistent with previously archived data for the same unique identification code; and

b. refusing communication of said service data when the number of times that received identifying data is not consistent with previously archived data for the same unique identification code exceeds a predetermined threshold.

58. (New) The method recited by Claim 55 further including the step of archiving identifying data received from a user for each unique identification code.

59. (New) The method recited by Claim 55 wherein said received service data is stored within the data storage element of the user's computer.

60. (New) The method as in Claim 1 further comprising the steps of:

requiring a user to provide identifying data that identifies the user;

deriving the user data that is communicated to the remote service provider, at least in part, from the identifying data that identifies the user;

archiving received identifying data in a data storage element of the remote service provider for each unique identification code; and

comparing the received identifying data for a given unique identification code with previously archived identifying data for the same unique identification code to determine whether they match each other.

61. (New) The method as in Claim 60 including the step of restricting transmission of said service data to the user's computer if said received identifying data for a given unique identification code does not match previously archived identifying data for the same unique identification code.

62. (New) The method as in Claim 31 further comprising the steps of:

requiring a user to provide identifying data that identifies the user;

deriving the user data that is communicated to the remote service provider, at least in part, from the identifying data that identifies the user;

archiving received identifying data in a data storage element of the remote service provider for each unique identification code; and

comparing the received identifying data for a given unique identification code with previously archived identifying data for the same unique identification code to determine whether they match each other.

63. (New) The method as in Claim 62 including the step of restricting transmission of said service data to the user's computer if said received identifying data for a given unique identification code does not match previously archived identifying data for the same unique identification code.

64. (New) The method as in Claim 35 further comprising the steps of:

requiring a user to provide identifying data that identifies the user;

deriving the user data that is communicated to the remote service provider, at least in part, from the identifying data that identifies the user;

archiving received identifying data in a data storage element of the remote service provider for each unique identification code; and

comparing the received identifying data for a given unique identification code with previously archived identifying data for the same unique identification code to determine whether they match each other.

65. (New) The method as in Claim 64 including the step of restricting transmission of said service data to the user's computer if said received identifying data for a given unique identification code does not match previously archived identifying data for the same unique identification code.

66. (New) A system for preventing piracy of a given software application, said software application having a unique identification code associated therewith, and said software application requiring service data to activate at least part of the functionality of said software application, said system comprising:

a user computer system on which a user desires to operate the software application, said user system being connected to a communications network to transmit user data and to receive said service data, said user data being derived at least in part from identifying data which identifies the user, and being derived at least in part from said unique identification code;

a remote service computer system connected to said communications network to receive user data transmitted over the communications network from the user computer system, said remote service computer system configured to performing the following steps:

archiving identifying data received from a user for each unique identification code if no such identifying data has previously been archived for such unique identification code;

comparing received identifying data associated with a unique identification code with previously archived identifying data corresponding to the same unique identification code if such identifying data has previously been archived;

selectively transmitting service data to the user's computer system over said communications network when no such identifying data has previously been archived for such unique identification code;

selectively transmitting service data to the user's computer system when it is determined that the received identifying data is consistent with previously archived data for the same unique identification code.

67. (New) The system as in Claim 66 wherein said service data is maintained by said remote service computer system in the data storage element used to archive said service data.

68. (New) The system as in Claim 66 wherein said service data consists, at least in part, of an activation code sequence to activate at least part of the functionality of the software application.

69. (New) The system as in Claim 66 wherein said service data is transferred by said remote service computer system without human intervention and received by said user computer system.

70. (New) The system as in Claim 66 wherein said remote service computer system manually transfers said service data from said remote service computer system to said user system.

71. (New) The system as in Claim 66 wherein said remote service computer system makes said service data available to said user from said remote service system, said user being able to download said service data into said user computer system.

72. (New) The system as in Claim 66 wherein said software application includes a program code sequence that identifies said software application stored on said data storage element of said user system, said software application additionally being responsive to a second program code sequence that activates at least part of the functionality of said software application, and which is transmitted to said user system via a communications network.

73. (New) The system as recited in Claim 68 wherein said service data includes at least one program code sequence that results in a promotional message that may be displayed to said user on said user computer system.